2

CSC-EPL-88/005

NATIONAL COMPUTER SECURITY CENTER

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT

OF

CLYDE DIGITAL SYSTEMS

DIALBACK

VERSION 1.5

29 August 1988

Approved for Public Release:
Distribution Unlimited

SUB-SYSTEM EVALUATION REPORT

CLYDE DIGITAL SYSTEMS

DIALBACK VERSION 1.5

NATIONAL
COMPUTER SECURITY CENTER

9800 SAVAGE ROAD
FORT GEORGE G. MEADE
MARYLAND 20755-6000

August 29, 1988

FOREWORD

This publication, the Subsystem Evaluation Report, Clyde Digital Systems, DIALBACK Version 1.5, is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the evaluation of Clyde's DIALBACK Version 1.5. Any requirements stated in this report are taken from *Department of Defense Trusted Computer System Evaluation Criteria*, dated December 1985.

Approved:

Eliot Sohmer August 29, 1988

Eliot Sohmer
Chief, Evaluations, Publications, and Support
National Computer Security Center

ACKNOWLEDGEMENTS

Evaluation Team Members

Stephen F. Carlton

Dana N. Stigdon

John W. Taylor

John L. Wyszynski

National Computer Security Center

9800 Savage Road

Fort George G. Meade, Maryland 20755-6000

Further Acknowledgement

SYSCOM

1000 Thomas Jefferson Street
Washington, D.C. 20007

For providing the test site

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Clyde DIALBACK[1] Version 1.5 is intended to serve as a user authentication mechanism for use with any VAX/VMS[2] systems. Since DIALBACK is a security subsystem rather than a complete system, it was not evaluated against an entire class in the *Department of Defense Trusted Computer System Evaluation Criteria*, dated December 1985, hereafter referred to as the "Criteria." Rather, it was assessed as to how well it performs user authentication and audit of dial-in events.

The evaluation team has determined that DIALBACK is a useful, effective authentication mechanism when configured as specified in this report.

Precaution must be taken in the administration of call-back security systems because they rely on the proper operation of generally unsecure telephone systems. Administrators of call-back security systems must therefore take great care in setting up such a system so that they do not create a situation that instills a false sense of security. The DIALBACK documentation, specifically "Appendix A", does an excellent job of pointing out the necessary precautions that must be taken in order to secure such a system.

[1] DIALBACK Version 1.5 is not presently supported for VAX/VMS Version 5.

[2] VAX and VMS are trademarks of Digital Equipment Corporation.

INTRODUCTION

Background

On January 2, 1981, the Director of the National Security Agency was assigned the responsibility for increasing the use of trusted computer security products within the Department of Defense. As a result, the DoD Computer Security Center was established at the National Security Agency. Its official charter is contained in DoD Directive 5215.1. In September 1984, National Security Decision Directive 145 (NSDD 145) expanded these responsibilities to include all federal government agencies. As a result, the Center became known as the National Computer Security Center (NCSC) in August 1985.

The primary goal of the NCSC is to encourage the widespread availability of trusted computer systems; that is, systems that employ sufficient hardware and software integrity measures for use in the simultaneous processing of a range of sensitive or classified information. Such encouragement is brought about by evaluating the technical protection capabilities of industry and government-developed systems, advising system developers and managers of their systems' suitability for use in processing sensitive information, and assisting in the incorporation of computer security requirements in the systems acquisition process.

The NCSC Computer Security Subsystem Evaluation Program

While the NCSC devotes much of its resources to encouraging the production and use of large-scale, multi-purpose trusted computer systems, there is a recognized need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class or level of the Criteria. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the NCSC's Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations. Managers should note that subsystems are not capable of protecting information with such assurance that classified information may be maintained on a system protected only by subsystems. Neither may subsystems be used to upgradethe protection offered by other complete security systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added on to other protection devices to add another layer of security but in no way may be used as justification for processing classified material.

Subsystems considered in the program are special-purpose products that can be added to existing computer systems to increase security and implement a security feature from the TCSEC. They also have the potential of meeting the limited security needs of both civilian and government departments and agencies. The scope of a computer security subsystem evaluation is limited to consideration of the subsystem and the attached system and does not address or attempt to rate the overall security of the processing environment. To promote consistency in evaluations an assessment is made of a subsystem's security-relevant performance in light of applicable standards and features outlined in the Criteria. Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, a summary of the evaluation report will be placed on the Evaluated Products List.

The report will not assign a specific rating to the product, but will provide an assessment of the product's effectiveness and usefulness in increasing computer security.

PRODUCT EVALUATION

Product Overview

The DIALBACK system is an add-on security product which is designed to provide user authentication for any VAX/VMS system by providing the capability to redial users at their pre-assigned telephone number. It consists of several software utilities that are designed to provide the security mechanisms. These utilities attempt to provide the ability to control dial-in lines and include database management utilities that configure the product. When DIALBACK is installed, these utilities are copied to the VMS system. Once there, they must be protected through the use of VMS security mechanisms.

After installation and incorporation of the patches found in the DIALBACK documentation, the system is designed to be used in the following manner. A DIALBACK user dials the VMS system from his modem. Once connected, DIALBACK prompts the user for his DIALBACK ID. DIALBACK then drops the connection and redials the user at a pre-assigned telephone number located in DIALBACK's database. Upon reconnection, DIALBACK prompts the user for his DIALBACK password and compares it with the password in DIALBACK's database associated with the re-dialed user. Therefore, DIALBACK attempts to insure that system access is only permitted from known, pre-authorized locations (i.e. telephone numbers) by DIALBACK authenticated users.

DIALBACK IDs, passwords, and re-dial telephone numbers are all set by the DIALBACK Administrator. It is assumed, though not required, that all DIALBACK IDs are the same as their VMS Username counterparts, for auditing and simplicity purposes. DIALBACK acts as a front-end authenticator and does not pass any information to VMS's LOGINOUT.

The DIALBACK Administrator is expected to set the appropriate Access Control Entries (ACEs) and User Identification Code (UIC) based protection mechanisms such that only authorized users are able to access the DIALBACK executables and databases.

Evaluation of Functionality

When configured correctly, DIALBACK can provide an additional authentication mechanism to VAX/VMS systems.[1] DIALBACK prompts for a user identifier when it receives a call. If DIALBACK receives a valid identifier, the product drops the connection with an appropriate message and proceeds to redial the user at the specified number. The user is then prompted to enter his DIALBACK password to gain access to the system. In addition, DIALBACK audits all login attempts and the success or failure of each redial.

Evaluation of Documentation

The DIALBACK documentation consists of three manuals, the *DIALBACK Installation Manual*, March 1987, the *DIALBACK User's Manual*, March 1987, and the *DIALBACK Reference Manual*, March 1987, the DIALBACK Version 1.5 Release Notes, and "Appendix A" (included in the Release Notes for incorporation in the *DIALBACK Reference Manual*). These documents, described below, contain a detailed description of the security features provided by DIALBACK. The documentation assumes a knowledge of the VAX/VMS operating system and each of the modems used to implement DIALBACK.

Installation Manual

This manual is intended for the system administrator. It contains the following chapters:

> INSTALLING DIALBACK FOR THE FIRST TIME
>
> This chapter gives detailed instructions concerning the initial installation of DIALBACK onto the system.

[1] See section entitled "Product in a Trusted Environment" for guidance on proper configuration.

INSTALLING A DIALBACK UPGRADE

This chapter gives detailed instructions concerning upgrading DIALBACK from one version to the next.

CONFIGURING DIALBACK FOR YOUR SYSTEM

This chapter is divided into a number of sections that explain the process of enabling/disabling DIALBACK, DIALBACK macros, the DIALBACK audit log, settable DIALBACK parameters, and DIALBACK flow control.

DIALBACK FILES

This appendix lists all DIALBACK files and the directories in which they must be located.

User's Manual

This manual is addressed to all DIALBACK users. It contains the following chapters:

USING DIALBACK

This chapter gives the DIALBACK user an introduction to the DIALBACK system and summarizes the step by step procedure for logging in.

GLOSSARY OF TERMS

This appendix defines terms the DIALBACK user may not be familiar with.

Reference Manual

This manual is intended for the DIALBACK System Administrator. It describes, in detail, the use of DIALBACK and its features. It contains the following chapters:

COMMAND LINE FORMAT

This chapter explains the commands to be used for configuring DIALBACK's database.

MACROS

This chapter explains what DIALBACK macros are and how to use them. It also explains the macros that come with DIALBACK and the process of creating custom macros.

CONFIGURING DIALBACK FOR UNSUPPORTED MODEMS

This chapter describes how to configure DIALBACK for those modems that are not supported by the supplied software.

DIALBACK PARAMETERS

This chapter explains each DIALBACK parameter and the process of setting and displaying them.

COMMAND REFERENCE

This chapter describes each DIALBACK command in detail.

APPENDIX A - DIALBACK SECURITY CONSIDERATIONS

This Appendix discusses the need for separate dial-in and dial-out lines, displaying a "Dialing Back" message for all access attempts, and auditing invalid DIALBACK IDs. It also provides macros that can be incorporated into DIALBACK in order to increase security.

THE PRODUCT IN A TRUSTED ENVIRONMENT

The Clyde DIALBACK product is designed to provide additional authentication on VAX/VMS systems by providing the capability to redial users at their specified phone numbers, thereby authenticating the user's location as specified by the system administrator. This capability can be useful and provide additional authentication functionality and assurance to a system, given that it is properly configured. DIALBACK, when configured[1] as stated below, provides this assurance.

SEPARATE DIAL-IN/DIAL-OUT LINES -- DIALBACK and, to a much greater degree, the telephone company must configure each telephone line as either dial-in or dial-out, but not both. This should be done by: configuring each dial-out modem such that it is in originate only (no auto answer) mode; restricting knowledge of the dial-out numbers; and requesting telephone lines that the telephone company has configured as dial-out only. Unless the telephone company configures each dial-out line such that they are not valid numbers for dialing (i.e. the telephone company will intercept the call with a "Number not in service" message)[2], there is no way DIALBACK can assure it has made a valid connection.

SIMILAR "DIALING BACK" MESSAGES FOR VALID AND INVALID USER IDS -- As shipped, DIALBACK displays a "Dialing Back" message for valid user IDs and no message for invalid user IDs. There is a patch in the DIALBACK documentation that will correct this such that either the "Dialing Back" message or no message will be displayed for both valid and invalid IDs.

AUDIT OF INVALID IDS -- As shipped, DIALBACK does not audit login attempts using invalid IDs. There is a patch in the DIALBACK documentation that will correct this such that use of both valid and invalid IDs is audited.

ADDING A DIALBACK PASSWORD -- As shipped, DIALBACK relies on the user's location for verifying that the user is who he says he is. In other words, DIALBACK authenticates a user's location as opposed to the user. There is a patch in the DIALBACK documentation that will correct this such that a user must enter both a valid DIALBACK ID, password, and be at the proper location before gaining access to the system login.

[1] This configuration can also be found stated in "Appendix A - DIALBACK Security Considerations" of the *DIALBACK Reference Manual.*

[2] This can be done through the use of a WATS line.

PRODUCT TESTING

Test Procedures

Testing represents a significant portion of a subsystem evaluation. The testing performed was primarily functional in nature; the security relevant characteristics of the product were compared against the claims of the vendor. The functional test suite of this product focused upon the following features: I&A and Audit. These security relevant features were identified in the *DIALBACK Reference Manual.*

This test suite consisted of several parts. The I&A mechanism was tested extensively, including attempts to subvert it and to bypass it entirely.

The Audit mechanism underwent extensive testing consisting of attempts to subvert or bypass the mechanism itself and attempts to corrupt audit data.

All tests were performed on a VAX/VMS Version 4 system.

Test Results

The test results described below are oriented toward providing the evaluation team's conclusions concerning the strengths and weaknesses of each security feature provided by DIALBACK.

When configured according to Appendix A of the *DIALBACK Reference Manual* and the configuration stated in this report, DIALBACK is able to provide additional authentication assurance to VAX/VMS systems. The evaluation team recommends that caution be taken in giving VAX/VMS privileges and only those users that require access are given access to the DIALBACK software, databases, and audit log.

Authentication

The Authentication mechanism was found to function properly; no access was granted to the system prior to entering a valid DIALBACK ID, successful redial, and entering the password associated with the DIALBACK ID The information used by the DIALBACK was, however, found to be modifiable by any user having certain privileges, access control entry, or User Identification Code access.

Audit

The audit records were found to contain the following information: time, date, event type, and user name. Audit records are created for all login attempts and the success or failure of each redial.

The team found that audit information could be damaged and changed by any user posessing the necessary VAX/VMS privileges or access control entries to gain access to the audit file. Because the audit data is in plain text, audit information is open to intelligible changes.

EVALUATOR'S COMMENTS

There is an inherent problem with all call-back security systems in that they rely on the proper operation of generally unsecure telephone systems. These telephone systems can easily be spoofed. It is also the case that certain features provided by the telephone company (such as call forwarding) could be used to exploit call-back security mechanisms. Modems are only so "smart" in that they can also be spoofed into believing they are "talking" to the telephone system. Administrators of call-back security systems must therefore take great care in setting up such a system so that they do not create a situation that instills a false sense of security. The DIALBACK documentation, specifically "Appendix A", does an excellent job of pointing out the necessary precautions that must be taken in order to secure such a system.

It should also be noted that such products also rely on the protection mechanisms provided by the host system. A DIALBACK system administrator should be familiar with VAX/VMS protection mechanisms (User Identification Code (UIC), Access Control Entries (ACE), and Priviledges) such that the DIALBACK software and databases can be protected from unauthorized access and modification.

☆U.S. GOVERNMENT PRINTING OFFICE 1989 622-419/10061

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS None
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; Distribution Unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL-88/005	5. MONITORING ORGANIZATION REPORT NUMBER(S) S231,241

6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center	6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (*City, State and ZIP Code*) 9800 Savage Road Ft. George G. Meade, MD 20755-6000		7b. ADDRESS (*City, State and ZIP Code*)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State and ZIP Code*)		10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.

11. TITLE (*Include Security Classification*)
[illegible] System Eval Report Clyde Digital Systems DIALBACK version 1.5

12. PERSONAL AUTHOR(S)
Carlton, Stepnen, Sigdon, Dana Nell, Taylor, John; Wyszynski, John

13a. TYPE OF REPORT Final	13b. TIME COVERED FROM ____ TO ____	14. DATE OF REPORT (*Yr, Mo, Day*) 880829	15. PAGE COUNT 20

16. SUPPLEMENTARY NOTATION

17. COSATI CODES			18. SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB. GR.	NCSC TCSEC authentication VAX/VMS DIALBACK Criteria audit

19. ABSTRACT (*Continue on reverse if necessary and identify by block number*)

The DIALBACK system is an add on security product which is designed to provide user authentication for any VAX/VMS system by providing the capability to redial users at their pre-assigned telephone number. It consists of several software utilities that are designed to provide the security mechanisms. These utilities attempt to provide the ability to control dial-in lines and include database management utilities that configure the product. When DIALBACK is installed, these utilities are copied to the VMS system. Once there, they must be protected through the use of VMS security mechanisms. This report documents the findings of the evaluation.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL [illegible]	22b. TELEPHONE NUMBER (Include Area Code) (301)859-4458	8b. OFFICE SYMBOL C12

EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE